EAI Endorsed Transactions
on Energy Web

Research Article EAI.EU

# An overview of security issues in Internet of Things based smart environments

M.V. Hari Vinayak[1] and T. Jarin[1,*]

[1]Jyothi Engineering College, Thrissur, India

## Abstract

Wireless Sensor Network (WSN) and Internet of Things (IoT) together have the potential to change the whole world into a smart planet. IoT technology has been a huge boon for a clean, green, and sustainable environment. This technology benefits numerous industries by improving connectivity and reducing energy wastage. IoT has the potential to make our environment more sustainable and help us to reduce pollution all across the globe. But due to limited resources in both these networks, it is very challenging to form a complete secure system. This survey paper examines the various security requirements and attacks possible in WSN and IoT. The paper surveys existing approaches like blockchain, fog/edge computing and machine learning to ensure security of IoT systems. The paper also evaluates the performance of common machine learning algorithms using IoT datasets.

**Keywords:** wireless sensor networks, Internet of Things, security threats, blockchain, fog computing, edge computing, machine learning.

Received on 24 February 2021, accepted on 13 June 2021, published on 15 June 2021



doi: 10.4108/eai.15-6-2021.170235

*Corresponding author. Email: jeroever2000@gmail.com

## 1.Introduction

WSNs consist of several sensor devices with sensing, computation, and wireless communication capabilities [1]. The network is usually composed of numerous wireless sensor nodes and a sink node. These nodes have limited storage and computational capabilities [2]. They are also limited in bandwidth and power. In order to collect the required data, these sensors become active when something is detected and then remain mostly idle for long periods of time. The nodes sense a physical phenomenon from the environment and then transfer the sensed data to the sink node. The idea of IoT was developed in parallel to WSNs. WSNs can be considered as a subset of IoT as the wireless sensor nodes can have internet access capabilities. In the case of an IoT system, all of the sensors directly send their data to the internet. Any device that connects to the internet can be considered an IoT device. By the year 2022, the total number of wireless sensors deployed is expected to reach 60 trillion [3]. WSNs and IoT systems can be used to monitor wildfire, earthquake, ocean, pollution, water quality, wildlife etc. and also can be used in human-related activities like military operations [4].

IoT has revolutionized the world and it has made very cost effective and efficient solutions in different areas [5]. Kevin Ashton introduced the concept of IoT in 1999 with reference to the supply chain management [6]. The ‘‘things or devices’’ in IoT are smart and uniquely addressable based on their communication protocols. An IP address is assigned to these devices so that they can send and receive data over a network. By the year 2025, IoT market is likely to grow to more than 75 billion devices. IoT is believed to have a dramatic impact on our lives and WSNs will be integrated into it. The vision behind IoT is to connect people and smart things at any time and in any place through any communication

network. Since IoTs are used in our day today lives, the security of these networks is of great concern. Also, both WSNs and IoT may be commissioned for mission-critical tasks. Many of the concepts of IoT networks come from WSNs and both have a wide range of applications. In IoT the sensing devices are smarter than WSN sensing nodes. In the case of WSNs the sensing devices merely gather and pass the sensed data to other nodes or to the sink node. IP addressing technique is used in IoT networks, whereas WSN uses special routing techniques to route the packets. The various IoT frameworks available for commercial use are Brillo/Weave from Google, ARM Bed from ARM and other partners, Azure IoT Suite from Microsoft, AWS IoT from Amazon, Calvin from Ericsson, HomeKit from Apple, Kura from Eclipse and SmartThings from Samsung.

## 2. Applications related to WSN integrated IoT environment

### 2.1. Environmental Monitoring

Air pollution is usually caused by led, carbon monoxide, sulphur dioxide and other heavy particles. It is the main cause for respiratory diseases, cancer, and Pneumonia. Quality of the air can be monitored by IoT devices and gathered data can be used to predict certain defects associated with air quality. The wildlife can also be monitored, and the results can be used for environmental protection.

### 2.2. Home Automation System

The devices like air conditioner, washing machine, windows, doors, lighting, refrigerator etc. can be controlled by home automation system from anywhere in the world. Employing IoT systems means greater control of home energy use via smartphones or tablets. These systems can be employed in countries where there are large number of elderly people. Using this, information about gas, water and power can be send to corresponding company for analysis and this increases the efficiency of the resources.

### 2.3. Smart Traffic Management System

Smart vehicles have integrated smart sensors and in a smart traffic management system these vehicles can communicate with each other. This system can be used to avoid collision, traffic management and to provide space for parking. The data from these vehicles can be processed in a cloud server for traffic prediction. An alarm can be raised if there is heavy traffic in certain streets. The system can also monitor traffic rules violators. Thus, IoT makes the overall traffic system smoother and more efficient.

### 2.4. Smart Health Monitoring System

Using health monitoring systems, a patient's sugar level, blood pressure and heartbeat can be sensed, and the data can be immediately sent to the doctor for diagnosis. The sensed parameters can also be transmitted to a cloud where it can be stored and analysed. Thus, aged, and chronic disease patients can be provided with special care using this system.

### 2.5. Smart Agriculture

The farming industry must employ new technologies like IoT to feed the growing population. IoT based smart agriculture assist the farmers to minimize wastage and improve productivity. The system uses automated irrigation system and monitors the crop field using sensors. The farmer is able to supervise his field from anywhere with the help of a smartphone. Smart agriculture gives several benefits to farmers like efficient use of water and fertilizers [7]. Smart agriculture using IoT helps in greatly reducing the agricultural waste that is a major pollutant in the environment.

### 2.6. Early Flood Detection and Avoidance

In order to reduce loss of life and property early detection of flood is necessary. By measuring the water level, humidity, temperature and flow level, a flood detection system can predict a flood situation. Various sensors like float sensor, flow sensor etc. can be used to monitor the level and flow of water [8].

### 2.7. Smart Supply Chain

Tracking of goods while on the road or in transit can be achieved using smart supply chain. It can also help the suppliers to exchange inventory information. Various parameters like temperature, pressure, and machine utilization can be communicated to a factory monitoring unit using an IoT enabled system. The system also modifies equipment settings so as to optimize the performance.

### 2.8. Social Life and Entertainment

IoT will dominate the world in terms of entertainment in the future. Entertainment industry is all about advertisements and IoT has the power to streamline ads too. Using the power of the IoT, entertainment giants can

analyse which ads to display, how the placement should be, and all the other possible aspects. Using this technology, you can predict customer response to a certain type of ad. This can improve the revenues received from the advertisements. Thus, with the help of IoT an ordinary world is transformed into a smart world in which everything can be accessed easily in less time and effort. Figure 1 shows the various application areas of IoT.

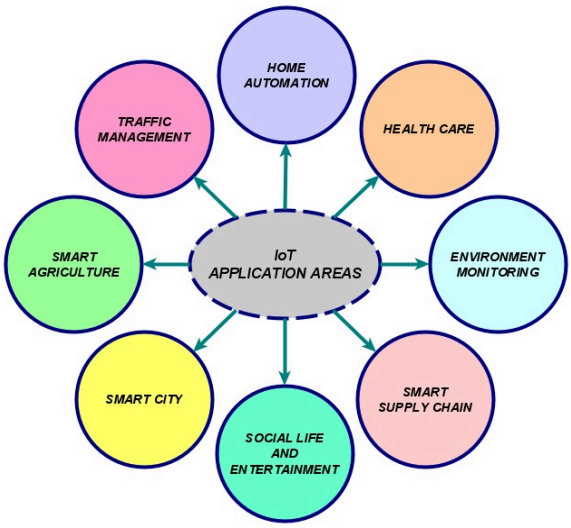


**Figure 1.** Application areas of IoT

## 3. Technological challenges and possible threats

Securing IoT systems presents several unique challenges as IoT devices are deployed in uncontrolled and often hostile environments [9]. The major technological challenges while building IoT are shown in figure 2. The technologies are growing rapidly, and this leads to threats and privacy issues. Security is important because the entire IoT network will be at risk if any of the node gets corrupted [10].

The network attack can be considered as an attempt of getting unauthorized access of the network [11]. The WSNs may be subjected to different kinds of passive or active attacks. The adversaries do not make any radio emissions in the case of passive attacks. They tap the communication lines to collect data and are usually hidden. An example of this is Eavesdropping. But in active attack, radio emissions are made by the adversary node. Denial-of-Service (DoS) attack is an example of this which causes nodes to drop data packets. The different layers of WSN architecture and various attacks occurring in these layers are shown in figure 3.

*Eavesdropping:* Eavesdropping is done by tapping the communication lines. The attacker must be in the vicinity of a node in order to access confidential data through eavesdropping (sniffing or snooping). Since the privacy is compromised, the WSN communication must be protected with an effective cryptographic mechanism.

*Node Capture (Tampering):* In this the attacker takes control of the device by a physical attack. This may expose the device's critical information including cryptographic keys and therefore the security of the whole network gets compromised.

*Man-in-the-middle attack:* In this, the attacker captures messages transmitted between two devices and then modifies the contents before sending them to the receiver. The attacker can add, drop, or modify the communication data and can also install network monitoring software.

*Jamming:* In this the attacker transmits signals at the same frequencies as that of WSN nodes. The jamming signal interferes with the authorized radio frequencies and causes noise in the carrier [12]. Thus, the signal-to-noise ratio gets reduced which hinders the correct reception of transmitted data.

*Collision Attack:* When different nodes start transmitting simultaneously then collision arises. When the WSN node transmits, the attacker also starts transmitting on the same channel. The data will be lost as a result of collision between two transmissions.

*Exhaustion:* In this the collision attack continues until the energy of WSN node gets exhausted. Repeat collisions means repeat re-transmissions of the same packets. The nodes become dead as the attack exhausts all its energy reserves.

*Unfairness:* In this attack the WSN node will not be completely disconnected from the network, but the messages will be delayed. This attack degrades the quality of service in the network.

*Link Layer Flooding:* In this, the attacker transmits excessive message packets to its neighbouring nodes. Eventually, it results in DoS as the batteries of target nodes get exhausted and this also consumes channel bandwidth.

*Traffic analysis and Monitoring:* In this, the attacker intercepts the messages and determines the type of ongoing communication in the network. Various nodes with specific activities can be identified which provide critical information about the network.

*Denial of Sleep:* Repeated handshaking or collision attacks eventually prevents a node from going into the sleep phase. This violates the sleep routines of the node which decreases the battery lifetime. So, this attack will affect the networks with battery powered devices.

*De-synchronization:* Attacks against TSCH (Time Synchronized Channel Hopping) time synchronization can be considered as an advanced form of collision attack. The messages are sent in the timeslots allotted to other nodes and this results in the collision of packets.

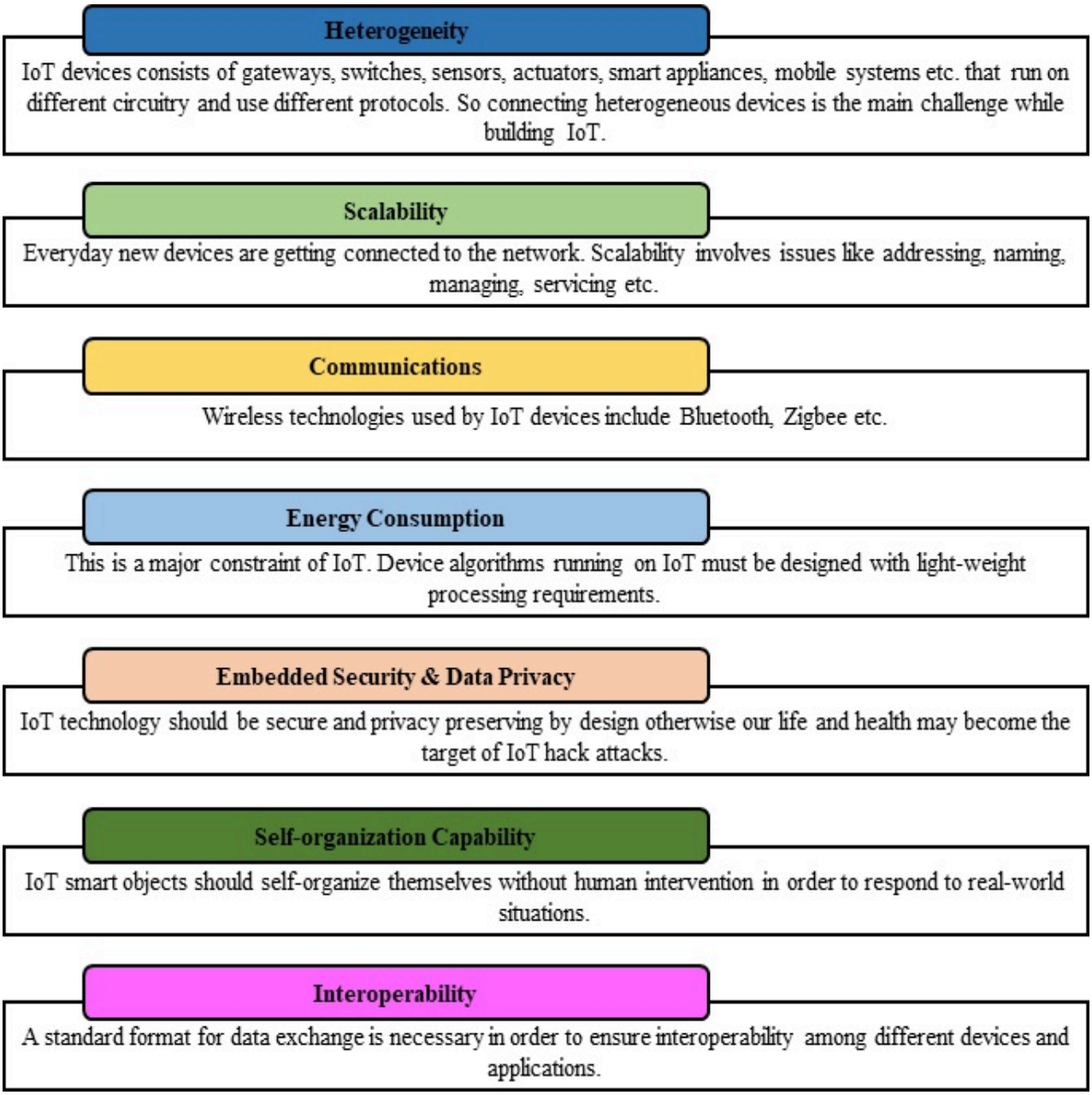


**Figure 2.** Major Technological Challenges of IoT

*6LoWPAN Exploit:* IPv6 over Low-power Wireless Personal Area Networks (6LoWPAN) is generally preferred to add smart devices to the internet. By fragmentation and reassembly of datagram fields, the protocol specifies the routing of data packets. In the case of fragment duplication attack, the attacker places his own fragments in the fragmentation chain. If there is no authentication mechanism, then the attacker can easily fool the receiver. It becomes very difficult for the receiver to distinguish genuine fragments from spoofed duplicates.

*Selective Forwarding Attack:* In this attack, adversary node transfers some of the packets and simply drops some other packets. If the attacker drops packets from a specific node or a set of nodes, then it is called selective forwarding attack. In another type, the corrupted node randomly skips routing certain messages.

*Blackhole Attack:* It can be considered as a particular type of selective forwarding attack in which the adversary node discards all the packets. If the node selectively discards a few packets, then it is termed greyhole attack.

*Sinkhole Attack:* In this, the attacker provides wrong routing information and makes the adversary node looks attractive to the neighbouring nodes. This way the adversary node can sink all the packets moving to the base station.

*Spoofing Attack:* In spoofing or impersonation attack, the attacker gains unauthorized service access to the network by sneaking the authentication credentials [13]. The attacker obtains full access to the network making it vulnerable. The various spoofing attacks include IP address spoofing, DNS server spoofing, ARP spoofing etc.

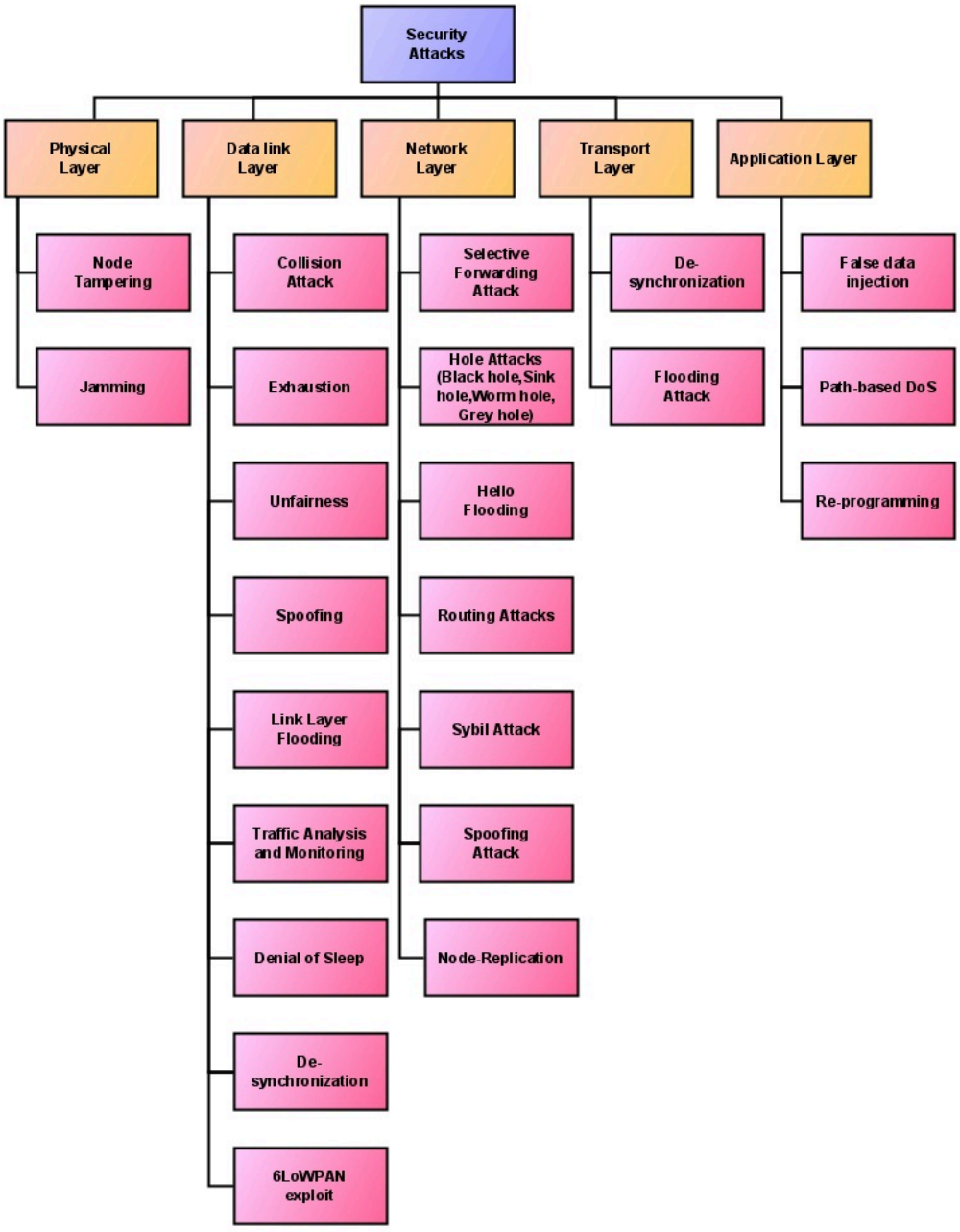


**Figure 3.** Security attacks on WSN integrated to IoT

*Wormhole Attack:* In this, the packets are transmitted in a faster way between two nodes by creating a channel or tunnel. This attack is achieved by collaboration of at least two nodes. The packets received at one location are tunnelled to another location and then replayed into the network from that location. If this attack is achieved using several nodes, then it is called Byzantine overlay network wormhole attack.

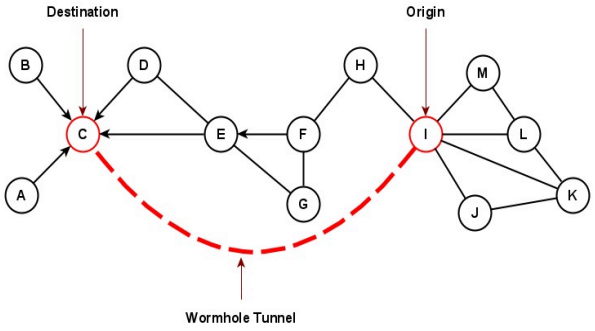


**Figure 4.** Wormhole Attack

*HELLO-flooding:* In order to inform of its presence, a node broadcasts "HELLO" messages to its one-hop neighbours. An adversary node can convince the legitimate nodes that it is a potential neighbour by sending HELLO packets with adequate power. The attacker can also create a high traffic by broadcasting a large number of useless messages.

*Sybil Attack:* By presenting multiple identities to legitimate nodes, a malicious node can create chaos in the network and the nodes receive conflicting routing paths. Thus, a node in Sybil attack deliberately and illegitimately produces numerous false or forge identities of sensor nodes in the WSN. This is done by either stealing legal identities of other nodes or creating new identities. This attack violates one-to-one mapping between entities and identity in WSN. Figure 5 provides a scenario of Sybil attack.

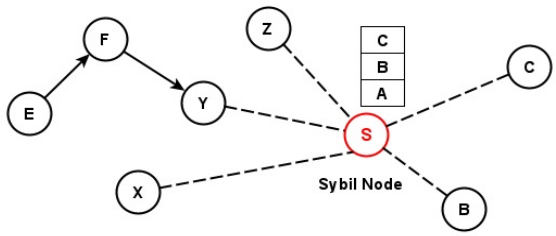


**Figure 5.** Sybil Attack

*Node-Replication:* In this, the attacker deliberately places copies of a node in many locations of the network. This creates confusion in the network and enables the attacker to disable functions or control the system [14].

*Routing Attacks:* In this attack, attackers create an improper route to transmit messages in the network. Messages are intentionally forwarded to the wrong paths and so this is also called misdirection attack. The routing tables of neighbouring nodes will be updated with wrong information and recorded packets can be used for replay attacks.

*Transport Layer Flooding:* An attacker can exhaust the energy of a node by transmitting several connection requests without ever fulfilling the connection. Also flooding the buffer with spurious messages exhaust the connection resources of legitimate node.

*False Data Injection:* Captured nodes can manipulate the final outcome of a measurement by deliberately injecting incorrect data into the network. As a result of this, IoT applications may become erroneous which affects the effectiveness of IoT networks.

*Path-based DoS:* In this the adversary overwhelms the nodes by flooding a network path using fake packets or replayed packets. All the nodes along this path gets affected due to this. In Distributed Denial of Service (DDoS), several malicious nodes from different geographic locations are used for attack. This type of attack can be easily launched using botnets.

*Re-programming:* If the program updating schedule of a network element is not kept secret, then this vulnerable time can be used by an attacker to send spurious messages. This can cause the node to become unstable.

## 4. Security techniques and approaches

The various techniques and solutions used for securing IoT environments may be classified into the following categories.

### 4.1. Security using blockchain.

The overall transparency, visibility, level of comfort and trust can be improved by blockchain and IoT technologies. The blockchain technology is like a distributed ledger. It has a ledger distributed over a network of nodes and data are shared among the peers [15]. Each node in the network gets a public key that is utilized by other nodes for encrypting the messages sent to a node. Such messages are read by a node using a private key. So, the nodes use one key for encrypting and another for decrypting the messages. The blockchain entries retain chronological order and are time stamped. A node broadcasts the signed transactions to its one-hop peers. This signing enables authentication and guarantees integrity. The receiving node verifies whether the transaction is valid and then retransmits it. Special nodes called miners are used to pack these transactions into a timestamped block. The hash of an earlier accepted block

is used to create another block in the chain. Figure 6 shows the various strengths of blockchain that can be utilized to secure IoT environment. The four basic pillars of blockchain technology are shared ledger, cryptography, consensus, and smart contract. No special permission is required for a user to become the part of blockchain network in the case of permission-less blockchain. But in permissioned blockchains the users should follow a set of rules [16]. Some platforms that support blockchain are Ethereum, Hyperledger fabric, Ripple etc. In the case of resource limited devices, a high level of security can be achieved using IOTA. It is a Distributed Ledger Technology like blockchain. Recently, Sun et al. [17] analysed the security of blockchain-enabled wireless systems and proposed security algorithms to overcome various attacks.

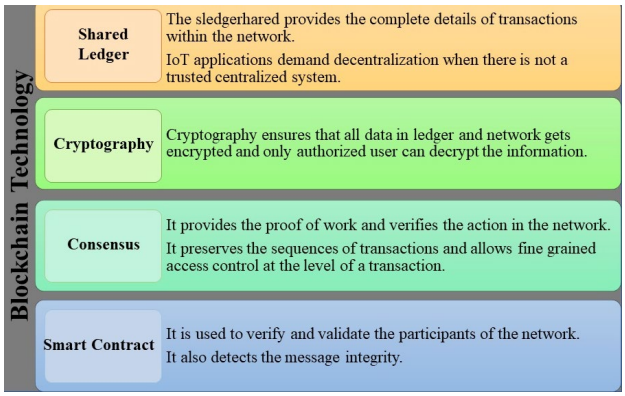


**Figure 6.** Blockchain technology strengths

## 4.2. Security using fog/edge computing.

We know that the enormous amount of data generated by IoT burdens the internet framework. The data from numerous sources from different geographical locations need to be stored, processed, and analysed. We know that the cloud offers an efficient solution to store and manage data and we can integrate IoT and cloud for processing, storing, managing, and securing data. The current cloud capability will not be able to process IoT applications that require faster processing [18]. So, the idea of fog computing was proposed which manages the data generated by IoT devices locally. For this it uses an architecture comprising of different layers as shown in figure 7. Both cloud computing and fog computing aids machine-to-machine communication and wireless connectivity. Improving the data security and increasing the efficiency of IoT devices are the main goals of fog computing. Low specification devices like switches and IP cameras can be fitted with fog system. A 20% decrease in the average response time for a user can be achieved by employing fog computing. Also, the data traffic between network edge and cloud can be reduced by 90% [19].

The key difference between edge computing and fog computing is the location of computing power and the way data are processed. In the case of fog computing, a decentralized computing architecture between source and cloud is used for processing and storing the data. But in edge computing, the computation facility is included in the data source device itself. So, fog/edge computing nodes can immediately process the high priority IoT data by means of this architecture. Now the main challenge is to effectively control this infrastructure and to distribute various resources to IoT devices since each node has limited processing and storage capabilities [20]. Thus, the computing resources should be efficiently managed. Accuracy issues are improved as a result of fog/edge computing as it detects and process data in real time. The various solutions that edge computing provides are as follows.

- In edge computing, there is no transfer of data from the source as it is processed in the device or local network itself and thus prevents data thefts.
- With the help of edge computing the data can be kept within an organization's country borders and thus guarantee compliance with data sovereignty laws.
- In edge computing, there is no need to transmit all the raw data to the cloud which requires large bandwidth. Only the summarized data after the initial processing at the edge nodes will be sent.
- Delay in responses of security systems is not desirable. In edge computing the nodes can analyse the anomalies and only the suspected data is sent to the data centres. This results in faster response times.
- Companies can expand their computing capability through a combination of IoT devices and edge computing. This presents an inexpensive way to scalability and versatility.

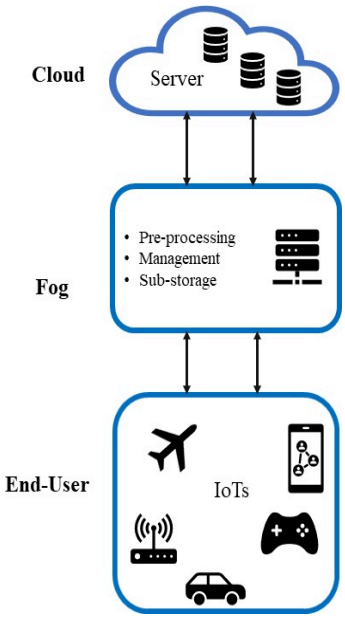


**Figure 7.** Cloud, fog, and edge computing

## 4.3. Security using machine learning.

Machine learning (ML) is a popular artificial intelligence (AI) algorithm that has applications in numerous fields. Researchers have studied the use of ML techniques in solving networking problems and in anomaly detection [21]. ML techniques can analyse and learn from previous experiences and can be used to forecast the expected outcome of a system. ML methods like supervised learning, unsupervised learning and reinforcement learning are employed to enhance security of networks [22]. In Supervised learning method, a prediction model is formed from the correlation between the input parameters and the expected output. Learning examples are used for training the algorithms at the initial stage. The supervised learning methods include SVMs (support vector machines), Naive Bayes, K-NN (K-nearest neighbour), NNs (neural networks), DNNs (deep neural networks) and Random Forest. These methods can be employed to detect network intrusion, spoofing attacks, malware detection and DoS attacks in various IoT devices. Unsupervised learning algorithms does not require labelled data and explore the similarity between unlabelled data. Then the algorithm classifies the data into various groups. Unsupervised ML techniques include clustering, anomaly detection and association mining. More complex processing tasks can be performed using unsupervised learning compared to supervised learning techniques.

Reinforcement Learning (RL) is defined as a ML method that is concerned with how software agents (model) should take actions in an environment in order to attain a complex objective. No specific outcomes are defined, and the agents learn from the feedback obtained after interaction with the environment. On the basis of actions performed rewards are obtained and the algorithm updates its policy in order to attain the highest reward. The training of reinforcement learning models is time consuming but once developed, the final models require less memory to perform.

Table 1. Potential ML techniques for IoT security

| Algorithm | Type | Complexity | Potential application in IoT Security |
|---|---|---|---|
| Naïve Bayes | Supervised | $O(nP)$ | Detection of intrusion / anomalies |
| SVM | Supervised | $O(n^2P + n^3)$ | Detection of intrusion / malware / DDoS |
| K-NN | Supervised | $O(nP)$ | Detection of intrusion / anomalies / DDoS |
| RF | Supervised | $O(n^2Pn_{trees})$ | Detection of intrusion / anomalies / DDoS / malware |
| K-Means | Unsupervised | $O(n^2)$ | Detection of intrusion / anomalies |
| Decision Tree | Supervised | $O(n^2Pn_{trees})$ | Detection of anomalies / intrusion / DDoS |
| Q-Learning | Reinforcement | $O(n^2)$ | Detection of DDoS attack / Authentication |
| NN | Supervised | $O(Pn_1 + n_1n_2 + \ldots)$ | Detection of intrusion / anomalies / DDoS |

The various RL techniques used by IoT devices include Q-learning, Dyna-Q, PDS (post decision state) and DQN (deep Q-network). Applications like authentication, antijamming offloading and malware detection can be effectively implemented using Q-learning. Some common ML based IoT security methods are summarized in Table 1[23], [24]. Here the computational complexity of the method is defined using the Big O notation. We assume that n is the number of training samples, P denotes the number of features, $n_{trees}$ denotes the number of trees in the case of algorithms based on various trees and $n_i$ denotes the number of neurons at layer i in a neural network. In the past, many researchers have studied the performance of ML methods on IoT datasets [25]. For analysis, several ML techniques were applied to these datasets and comparison results were obtained on the basis of performance. Figure 8 shows how the accuracy results vary for five common ML algorithms. Accuracy

denotes the portion of correctly predicted instances taking into consideration the total number of predictions [26]. It is found that the performance of Naïve Bayes and Logistic Regression decreases when the size of dataset increases. But the performance of Decision tree, Random Forest and KNN is not affected by the increase in size of data set. None of the methods works best in all the cases and a method should be selected on the basis of training size, number of features, computational complexity, type of features etc. Schneible et al. [27] proposed a system for identifying anomalies in edge computing by integrating simulated neural networks. The proposed scheme achieves improved bandwidth, latency, and computation power efficiency. The performance of fog/edge computing applications can be significantly improved using ML techniques and it is also widely applied in healthcare domain.

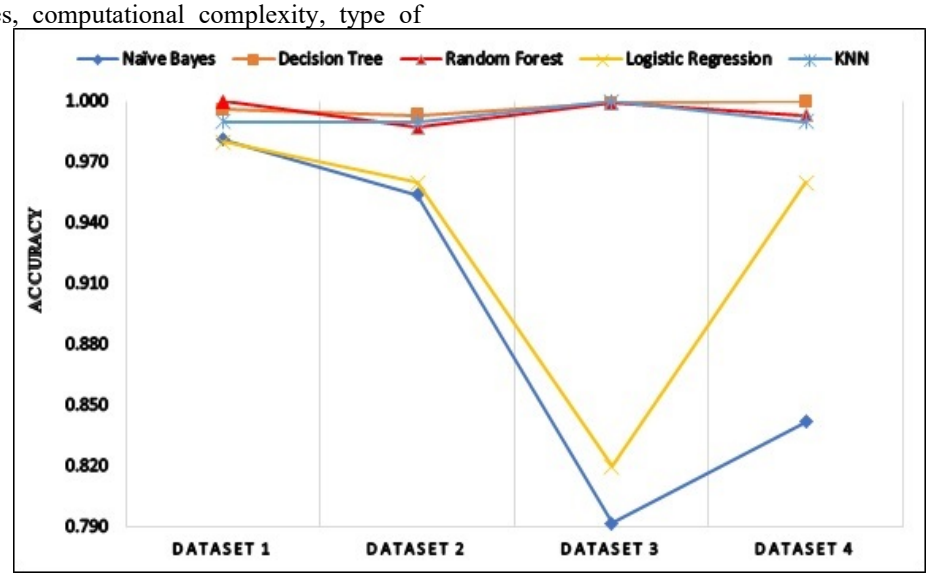


**Figure 8.** Accuracy of a few well-known supervised ML methods

## 5. Conclusion

In this survey, we discussed about WSN and IoT based networks and the various possible attacks and security requirements. Due to the rapid growth in IoT applications, there occurs several threats in security and privacy which needs to be addressed. The paper reviews various security threats concerning WSNs in IoT context and also the defending strategies against these attacks. We also explored certain solutions including fog computing, edge computing and machine learning. The advancement in machine learning has resulted in the development of various powerful techniques that can be used to improve IoT security. Although there are challenges involved, building a more sustainable environment is possible with IoT and it is set to push the future of environment preservation to the next level. There is still a significant work to be done in order to secure IoT systems as these systems are being increasingly deployed in industrial systems, health care, military operations, and many other sensitive areas.

## References

[1] K. Romer and F. Mattern, ‘‘The design space of wireless sensor networks,’’ IEEE Wireless Commun., vol. 11, no. 6, pp. 54–61, Dec. 2004.
[2] A. Kumar, M. Zhao, K. Wong, Y. L. Guan and P. H. J. Chong, "A Comprehensive Study of IoT and WSN MAC Protocols: Research Issues, Challenges and Opportunities," in IEEE Access, vol. 6, pp. 76228-76262, 2018.
[3] I. Butun, S. D. Morgera, and R. Sankar, “A survey of intrusion detection systems in wireless sensor networks,” IEEE communications surveys & tutorials, vol. 16, no. 1, pp. 266–282, 2014.
[4] I. Butun, P. Österberg and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures," in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 616-644, Firstquarter 2020.
[5] M. Abomhara and G. M. Køien, “Security and privacy in the internet of things: Current status and open issues,” in Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on. IEEE, pp. 1–8, 2014.
[6] K. Ashton, ‘‘Internet of Things,’’ RFID J., vol. 22, no. 7, pp. 97–114, 2009.
[7] R. Chowdhury, Top 20 Best Internet of Things Projects (IoT Projects) That You Can Make Right Now. Accessed: Oct. 2019.
[8] H. Larthani, A. Zrelli, and T. Ezzedine, ‘‘On the detection of disasters: Optical sensors and IoT technologies,’’ in Proc. Int. Conf. Internet Things, Embedded Syst. Commun. (IINTEC), Hammamet, Tunisia, pp. 142–146 Dec. 2018.

[9] A. Balte, A. Kashid, and B. Patil, “Security issues in internet of things (iot): A survey,” International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, no. 4, 2015.
[10] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues and Y. Park, "Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges," in IEEE Access, vol. 8, pp. 3343-3363, 2020.
[11] I. Andrea, C. Chrysostomou and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," 2015 IEEE Symposium on Computers and Communication (ISCC), pp. 180-187, Larnaca, 2015.
[12] T. Borgohain, U. Kumar, and S. Sanyal, “Survey of security and privacy issues of internet of things,” arXiv preprint arXiv:1501.02211, 2015.
[13] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, “Classifying rfid attacks and defenses”, Information Systems Frontiers, 12(5):491–505, November 2010.
[14] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques," in IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2671-2701, thirdquarter 2019.
[15] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," in IEEE Access, vol. 6, pp. 32979-33001, 2018.
[16] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," in IEEE Access, vol. 7, pp. 82721-82743, 2019.
[17] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, and M. A. Imran,“Blockchain-enabled Wireless Internet of Things: Performance Analysis and Optimal Communication Node Deployment,” IEEE Internet of Things Journal, 2019.
[18] K. H. Abdulkareem et al., "A Review of Fog Computing and Machine Learning: Concepts, Applications, Challenges, and Open Issues," in IEEE Access, vol. 7, pp. 153123-153140, 2019.
[19] B. Varghese, N. Wang, D. S. Nikolopoulos, and R. Buyya. ‘‘Feasibility of fog computing,’’ 2017,
[20] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125-1142, Oct. 2017.
[21] M. Wang, Y. Cui, X. Wang, S. Xiao, and J. Jiang, ‘‘Machine learning for networking: Workflow, advances and opportunities,’’ IEEE Netw., vol. 32, no. 2, pp. 92–99, Mar./Apr. 2018.
[22] L. Xiao, X. Wan, X. Lu, Y. Zhang and D. Wu, "IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?" in IEEE Signal Processing Magazine, vol. 35, no. 5, pp. 41-49, Sept. 2018.
[23] F. Hussain, R. Hussain, S. A. Hassan and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1686-1721, thirdquarter 2020.
[24] M. K. Pakhira, "A Linear Time-Complexity k-Means Algorithm Using Cluster Shifting," 2014 International Conference on Computational Intelligence and Communication Networks, Bhopal, pp. 1047-1051 2014.
[25] V. Khadse, P. N. Mahalle and S. V. Biraris, "An Empirical Comparison of Supervised Machine Learning Algorithms for Internet of Things Data," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, pp. 1-6, 2018.
[26] A. A. Diro, N. Chilamkurti, Distributed attack detection scheme using deep learning approach for internet of things, Future Gen. Comput. Syst. pp. 761–768, 2018.
[27] J. Schneible and A. Lu, ‘‘Anomaly detection on the edge,’’ in Proc. IEEE Mil. Commun. Conf. (MILCOM), pp. 678–682, Oct. 2017.